**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT).

(51) International Patent Classification 5 : H04Q 7/04 — A1

(11) International Publication Number: WO 94/30023

(43) International Publication Date: 22 December 1994 (22.12.94)

(21) International Application Number: PCT/GB94/01295

(22) International Filing Date: 15 June 1994 (15.06.94)

(30) Priority Data:

| | | |
|---|---|---|
| 9312320.6 | 15 June 1993 (15.06.93) | GB |
| 9313772.7 | 2 July 1993 (02.07.93) | GB |
| 9314096.0 | 8 July 1993 (08.07.93) | GB |

(71) Applicant *(for all designated States except US)*: CELLTRACE COMMUNICATIONS LIMITED [GB/GB]; Poplars Farm, Crouch Lane, Winkfield, Berkshire SL4 4TL (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MICHAELS, Wayne, David [GB/GB]; Poplars Farm, Crouch Lane, Winkfield, Berkshire SL4 4TL (GB). TIMSON, Anthony, Richard [GB/GB]; 39 Carnelite Road, Harrow-Weald, Middlesex HA3 5LT (GB). DERVAN, Aden, William [GB/GB]; 90 Sedlescombe Road, Fulham, London SW6 1RD (GB).

(74) Agents: WARREN, Keith, Stanley et al.; Baron & Warren, 18 South End, Kensington, London W8 5BU (GB).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

**Published**

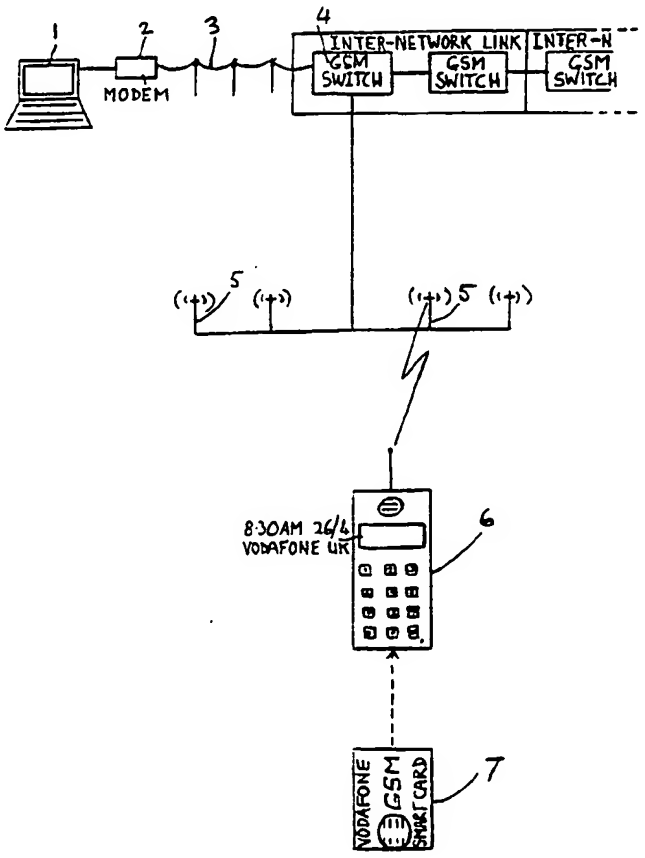
*With international search report.*

*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: TELECOMMUNICATIONS SYSTEM

(57) Abstract

In a telecommunications system such as a global mobile telephone network in which each subscriber unit includes a Subscriber Identity Module (SIM card), each SIM card has fixed memory locations (22), to which data can be addressed over the air. Some of the locations (22) can not be overwritten from the subscriber unit but can be accessed therefrom on the entry of short simple codes, each associated with one of the locations. Further fixed memory locations (24) can be read over the air only when the subscriber enters a personal identification number. Locking control files (27, 28) are used to control read/write access to the locations (22, 24) respectively.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|---|---|---|---|---|---|
| AT | Austria | GB | United Kingdom | MR | Mauritania |
| AU | Australia | GE | Georgia | MW | Malawi |
| BB | Barbados | GN | Guinea | NE | Niger |
| BE | Belgium | GR | Greece | NL | Netherlands |
| BF | Burkina Faso | HU | Hungary | NO | Norway |
| BG | Bulgaria | IE | Ireland | NZ | New Zealand |
| BJ | Benin | IT | Italy | PL | Poland |
| BR | Brazil | JP | Japan | PT | Portugal |
| BY | Belarus | KE | Kenya | RO | Romania |
| CA | Canada | KG | Kyrgyzstan | RU | Russian Federation |
| CF | Central African Republic | KP | Democratic People's Republic of Korea | SD | Sudan |
| CG | Congo | | | SE | Sweden |
| CH | Switzerland | KR | Republic of Korea | SI | Slovenia |
| CI | Côte d'Ivoire | KZ | Kazakhstan | SK | Slovakia |
| CM | Cameroon | LI | Liechtenstein | SN | Senegal |
| CN | China | LK | Sri Lanka | TD | Chad |
| CS | Czechoslovakia | LU | Luxembourg | TG | Togo |
| CZ | Czech Republic | LV | Latvia | TJ | Tajikistan |
| DE | Germany | MC | Monaco | TT | Trinidad and Tobago |
| DK | Denmark | MD | Republic of Moldova | UA | Ukraine |
| ES | Spain | MG | Madagascar | US | United States of America |
| FI | Finland | ML | Mali | UZ | Uzbekistan |
| FR | France | MN | Mongolia | VN | Viet Nam |
| GA | Gabon | | | | |

# TELECOMMUNICATIONS SYSTEM

This invention relates to a telecommunications system. In particular, but not exclusively, it relates to a mobile communications system such as a cellular mobile radio or telephone system.

A recent innovation in such systems has been the introduction of Subscriber Identity Modules (SIM cards). These are integrated circuit cards which can be releasably inserted into a mobile telephone and which contain in memory the subscriber's identity, i.e. his telephone number. These known SIM cards also have a rolling buffer which can store a certain number of alphanumeric characters. The buffer facilitates the so-called Short Message Service (SMS) in which a message for a subscriber or for a specified group of subscribers can be broadcast over the air, as an advanced form of radiopaging. Messages can be received by a mobile telephone whenever it is idle or on stand-by. However, if a message is received which would overfill the buffer, data is lost on a first-in-first-out basis.

It is an object of the invention to provide a more efficient and remotely reconfigurable SIM card.

From one aspect, the present invention consists in a telecommunications system comprising at least one host station and a plurality of subscriber units, the or each host station being operable to transmit a message to at least one of the subscriber units, and each subscriber unit having a multiplicity of fixed memory locations and means responsive to the detection of the message to store the message in a selected one of the fixed memory locations which can not be overwritten from the subscriber unit, but which can be accessed from the subscriber unit when required.

In this description and the accompanying claims, a "fixed" memory location means a location into which data can be written, and excludes first-in-first-out or circular

buffers. Overwriting of all the data in certain "fixed" memory locations may occur in contrast to the first-in-first-out loss of data experienced with current SMS buffers.

Thus, for example, a set of telephone numbers, each with an identifying alphanumeric tag, can be transmitted to the SIM card, allowing users easy access to commonly used services such as hotels, car hire or airline reservations. This feature is known as a Value Added Service Directory.

A message may be retrievable by the subscriber on the entry of simple, short codes into the subscriber unit, each memory location corresponding to a particular code. A message may include a telephone number and, once stored, may be able to be overwritten over the air. Preferably, the or each host station is operable to transmit a request for information stored in a subscriber unit. The information may be included in a message and it may also include information which is stored in a secure memory location, accessible only when the subscriber enters a personal identification number (PIN number). The information may include credit details relevant to the subscriber, for example, a credit card number of credit status, thus greatly facilitating credit card transactions carried out over the telephone. Using this feature of the invention, a credit account holder avoids having to dictate his account details and need only enter the mandatory PIN number.

The host station may be operable to transmit instructions to lock and/or unlock a memory location at the subscriber unit. It may be operable to transmit instructions to run a program stored in memory locations at the subscriber unit. The host station may be operable to transmit files containing functional data and/or files containing non-functional data to the subscriber unit.

The messages, requests for information and the instructions being transmitted may be in a specific format which the subscriber unit is able to distinguish from other

formats. The specific format may be made secure against interception.

In a preferred embodiment, the subscriber unit comprises a mobile radio or telephone and an integrated circuit card which can be removably connected to the radio/ telephone. The integrated circuit card may contain the memory locations and may contain means for distinguishing the specific format from other formats. The card may contain means for distinguishing between the messages, requests for information and instructions. The card may also contain the means for storing the messages and means for acting on the requests and instructions.

From another aspect, the invention consists in a module for controlling a subscriber unit in a telecommunications system, comprising a multiplicity of fixed memory locations and means responsive to the detection of a message transmitted remotely thereto to store the message in a selected one of the fixed memory locations, and being adapted for removable connection to a transceiver of the subscriber unit.

At least one of the fixed memory locations may be protected from overwriting by the subscriber. The module or card may include means for rendering any or all of said fixed memory locations accessible or inaccessible by either the subscriber or the host station. The card may include a directory structure within which files can be stored.

The invention is particularly applicable to global telecommunication systems in which the mobile cellular telephone networks of various countries or areas communicate using a common standard. An example of such a global system is GSM (Global System for Mobile Communications) currently operating in Europe. However the invention is not limited to global systems and could be applied to a single national cellular network or even to a fixed land-linked network.

An embodiment of the invention will now be described by way of example with reference to the accompanying

drawings in which:-

Figure 1 shows the transmission of messages to a subscriber unit in a system according to the invention;

Figure 2 shows a process in which a subscriber unit transmits a message and requested information;

Figure 3 is a block diagram showing elements of a module shown in figures 1 and 2;

Figure 4 shows details of one of the blocks shown in figure 3; and

Figure 5 is a flowchart showing the operation of the module shown in figures 1 to 4.

Figure 1 illustrates an SMS distribution path according to the invention. In the prior art, the short messages have usually been directed to a single subscriber or a specified group of subscribers such as a sales team.

However, GSM also supports a feature known as Cell Broadcast in which messages can be sent to all the subscribers in a particular area. In the embodiment of the invention illustrated, a message consists of the telephone number of an advertiser and an alphanumeric tag to identify the advertiser.

An operator enters the message into a terminal 1. The message is then coded into a secure format known as an Embedded Command Stream (ECS) and sent via a modem 2 and a fixed line 3 to a local GSM switch 4. According to its delivery address, the message is delivered to any or all of the other switches within that network, or even across networks.

The switch 4, which in this example is in the geographical area to which the message is to be transmitted, delivers the message to a number of cellsites 5. The cellsites 5 are the base transceiver stations of the GSM network.

Each cellsite 5 then broadcasts the message to a group of transceivers or mobile telephones, hereinafter referred to as "mobiles". If Cell Broadcast is used, the group consists of all mobiles within the geographical area at the

time of the broadcast.

A selected mobile 6 receiving the message transmits a confirmation of receipt back to its respective cellsite 5. From now on, until an update situation, the system will not contact this mobile 6 again.

The mobile 6 recognises the message as SMS data and passes it to a SIM card 7, which is a small self-contained microprocessor, held in a slot in the mobile 6. The SIM card 7 in turn recognises the ECS using special hardware and software and stores the message in memory in such a way that it may not be overwritten by the subscriber. Known SIM cards contain a large number of fixed memory locations in which the subscriber can store frequently dialled numbers and corresponding alphanumeric tags. The SIM card 7 of the invention stores the message in one of these locations, and then carries out a write protect operation. The locations dedicated to storing write protected messages may be designated by code numbers relating to a particular category of advertiser. Thus, for example, car hire company telephone numbers can be stored in location 01, hotel reservations in location 02 and so on.

Figure 2 shows a call placing process in which a subscriber communicates with an advertiser. The subscriber, remembering that the car hire company's number is in location 01 as shown at 8, keys in a short code corresponding to the location, such as 01#. The mobile 6 then interrogates the SIM card 7 to retrieve the telephone number from the location. The SIM card 7 provides both the number and the alphanumeric tag giving the company's name and displays it to the subscriber. The user confirms that he wishes to proceed by pressing SEND.

Next, the mobile obtains a voice channel through which the call proceeds to the dialled number. The GSM system automatically handles intra-network and inter-network hops. At this point the subscriber can hold a voice conversation with the company.

Providing the correct equipment has been installed at

the company, as soon as the call is answered, subscriber identity information read from the SIM card 7 gives the company immediate customer billing details such as a name and address.

The SIM card 7 also contains information detailing the subscriber's credit account. This information is held in a separate, secure memory location, accessible only when the subscriber enters a mandatory PIN number, known only to himself, thus confirming that the mobile has not been stolen or lost. When the subscriber has confirmed his car hire deal, he enters the PIN number into the mobile 6, requesting the credit information from the SIM card 7. The SIM card 7 supplies the information and the mobile uses existing voice/data techniques to transmit the information to the company, in a format secure against detection by fraudsters. The sale is confirmed by the company or its equipment and the call is terminated.

In this example, it is also possible to obtain a telephone or fax number from the operator-assisted directory enquiries system without the subscriber having to manually enter the number into the communications terminal which he desires to use.

To use this feature, the subscriber calls network directory enquiries and gives the name of the person, company or service of which he wishes to ascertain the telephone number, as well as any additional information requested by the operator answering the call. The operator then locates the number, confirms it and enquires as to whether the number is to be transmitted verbally, transferred over SMS into a given memory location of the subscriber's SIM card or both.

If the subscriber chooses a SIM update, the voice call is terminated and the operator initiates the SMS process by entering a sequence into a computer or pressing a dedicated button. The telephone number is then encoded into an ECS message at the despatch centre and is posted across the network to the subscriber's communications terminal, which

transmits a confirmation to the despatch centre. Thus the retry mechanism, which operates until such a confirmation is received, is suspended.

The communications terminal recognises the message as SMS data, passes it to the SIM card, and if capable, displays a "message received" banner. The SIM card in turn recognises the ECS using special hardware and software, and decodes it accordingly. The number, and any associated alphanumeric tag, which would normally consist of the name of the person or company, are recovered together with the memory location in which they are intended to be stored. The number and name-tag are then written to that location and are write-protected if requested by the subscriber, the overwrite protection being encoded into the message at source.

Subsequently, the subscriber attempts to place a call to the number in the known memory location by keying in the memory location number. The SIM card passes the telephone or fax number to the communications terminal on demand, and upon receipt of the subscriber's confirmation, the communications terminal sets up the call to the desired number.

Figure 3 shows the electronic structure of the SIM card 7. The card communicates with the mobile to which it is connected via an input/output (I/O) manager 15, preferably using the protocol ISO 7816 T=0. A filter 16 receives incoming data from the I/O manager and detects any ECS messages from among the short messages received. The ECS messages are sent directly to an extended erasable read only memory ($E^2$ROM) 17, which is preferably a "flash" $E^2$ROM. Data can also be output from the $E^2$ROM directly to the I/O manager 15. The remaining blocks shown in figure 3 are standard components of a SIM card.

Figure 4 shows how the $E^2$ROM is organised. A root directory 18 contains a SIM administration and identifier 19, a GSM directory and network data 20, and a telecom directory 21.

The telecom directory in turn contains memory locations as follows: "abbreviated dial numbers" 22, "capability configuration" 23, "short messages" 24, "fixed dial numbers" 25, and "charging counter" 26. Each block represents a plurality of memory locations. The frequently dialled numbers and corresponding alphanumeric tags are stored at locations 22.

The "abbreviated dial numbers" locations 22 and the "short messages" locations 24 each have an associated locking control file 27, 28 respectively. The locking control files constitute means for read/write protecting and removing read/write protection from their associated memory locations. The locking control files 27, 28 will typically be in the telecom directory 21 as shown, however they can be located elsewhere such as in an administration directory.

Figure 5 is a flowchart illustrating the operation of the SIM card 7, which uses the specially fabricated hardware and software which has been described above to implement the operations illustrated. At lozenge 9, messages, requests, and instructions having ECS are distinguished from those without. Each of these ECS types consists of a data stream headed by a command which is one of at least four types: write commands for the messages, read commands for the requests for information, attribute commands for lock or unlock instructions and run commands for instructions to run a program.

The command and data types are decoded at box 10 and acted on in one of the four paths 11-14.

Path 11 handles the write commands to store messages starting at a location specified therein. Path 12 handles the read commands; again, the requests for information contain a location to be accessed first. Successive locations are read and the data stored in a buffer until the required amount of data has been read. The data in the buffer is then encoded into the ECS format and despatched from the mobile using SMS to the calling party.

In path 13, attribute commands are used to lock or unlock specified memory locations and render them accessible or inaccessible, either to calling parties or to the subscriber. In path 14, run commands cause a program stored in the SIM card to be run.

The basic ECS system is expandable to up to 255 internal shell commands of which write, read, lock/unlock and run are four examples. The specific protocol used for the transfer of information is not fixed and could be ISO7816 T=0 or any other suitable protocol.

The internal shell commands are a supplement to the ability of the system to create external file objects within the SIM card 7. The file objects are of two types: Application Data File Programs (ADFP's) containing functional data which can be executed by the SIM card processor and can self modify if required and Application Data Files (ADF's) containing non-functional data which does not have these capabilities. Existing ADF(P)'s can be modified over-the-air enabling advanced facilities such as personalisation, re-personalisation or downloadable phone book.

The SIM card 7 has a directory structure, similar to that of a computer disk, and new ADF(P)'s can be downloaded into any directory over the air. Also over the air, directories can be created, deleted and modified, multiple tree directory operations can be carried out and ADF(P)'s that are no longer required can be deleted. The amount of ADF(P) data which can be downloaded is limited only by the size of the $E^2$ROM memory of the card.

The invention, as described, greatly extends the applications of SIM cards. For example, using the Value Added Services Directory, subscribers can book hotels and airline seats over their mobiles quickly and easily.

An additional advantage of this feature of invention is that the geographical distribution of messages to cards in a specific area such as the South of France is facilitated. Thus advertisers can direct their messages to

all mobile subscribers in the specific area. This is particularly useful when subscribers "roam" from one area to another and have no knowledge of local services.

The directory enquiries download enables contact telephone or fax numbers to be delivered to a subscriber's communications terminal without any intervention by the subscriber. The process of manually entering a number whilst engaged in a call to the operator is often dangerous, especially when the subscriber is driving.

The ability of the system to download ADF(P)'s means that additional services can be added to the SIM card over the air while maintaining total compatibility with the existing cellular system. Thus the SIM card could acquire the functions of a credit card, passport, driving licence, car park pass, membership card and so on, becoming a multi-service card. Also, dynamically updatable services can be added which require a different process to be run each time a service is accessed.

Once the card has extra services on it, it can be used outside of the mobile phone environment if desired as a standalone item. This can be read from or written to by a dedicated piece of hardware, such as a point of sale machine. If desired, the new services can be deleted, however the card will never lose its mobile phone SIM capability. In addition, if the card has extra services, they will continue to function even if the subscriber has been disconnected from the mobile phone network, unless otherwise desired.

Modifications are possible without departing from the scope of the invention.

For example, the SIM card can be trained only to receive messages detailing services relevant to the subscriber's needs.

CLAIMS

1. A telecommunications system comprising at least one host station (1) and a plurality of subscriber units (6,7), the or each host station being operable to transmit a message to at least one of the subscriber units, and each subscriber unit (6,7) having a multiplicity of fixed memory locations (22) and means responsive to the detection of the message to store the message in a selected one of the fixed memory locations which can not be overwritten from the subscriber unit (6,7), but which can be accessed from the subscriber unit when required.

2. A system as claimed in claim 1, wherein at least one of the subscriber units (6,7) comprises a transceiver (6) and an integrated circuit card (7) or other module having the fixed memory locations (22), and means responsive to the detection of a message by the transceiver to route it to the selected fixed memory location, said module being removably connected to the transceiver.

3. A system as claimed in claim 1 or 2, wherein each memory location (22) is associated with a simple, short code, and the subscriber unit (6,7) includes means responsive to the entry into the unit of each code to retrieve data from the associated memory location.

4. A system as claimed in any preceding claim, wherein the or each host station (1) is operable to overwrite the message stored in the fixed memory location (22) at each subscriber unit (6,7).

5. A system as claimed in any preceding claim, wherein the or each host station (1) is operable to transmit a request for information stored in a fixed memory location (24) within a selected one of the subscriber units (6,7), and each subscriber unit contains means responsive to such a request for retrieving and transmitting the information.

6. A system as claimed in claim 5, wherein the means responsive to the request is actuated only on the entry of a personal identification number (PIN number) into the

subscriber unit (6,7).

7. A system as claimed in any preceding claim, wherein the subscriber unit (6,7) has a multiplicity of further fixed memory locations which can be overwritten from the subscriber unit (6,7).

8. A system as claimed in any preceding claim, wherein each subscriber unit (6,7) includes means (27, 28) responsive to an instruction transmitted from the or each host station (1) selectively to enable or prohibit said further fixed memory locations to be overwritten from the or each host station (1) or from the subscriber unit (6,7).

9. A system as claimed in any preceding claim, wherein each subscriber unit (6,7) includes means responsive to an instruction transmitted from the or each host station (1) to run a program stored in said fixed or further fixed memory locations at the subscriber unit (6,7).

10. A system as claimed in claim 8 or 9, when dependent upon claim 5, wherein the or each message, request for information and instruction transmitted is in a specific format, and the subscriber unit (6,7) includes means (16) for recognising the specific format.

11. A system as claimed in one of claims 3 to 10, when dependent upon claim 2, wherein the module (7) includes the means responsive to the detection of a message to store the message in a selected one of the fixed memory locations, and/or the means responsive to the entry of a simple short code to retrieve data from the associated memory location, and/or the means responsive to a request for information to retrieve and transmit the information, and/or the multiplicity of further fixed memory locations which can be overwritten by the subscriber, and/or the means for selectively enabling or prohibiting said further fixed memory locations to be overwritten, and/or the means for running a program, and/or the means for recognising the specific format.

12. A module (7) for controlling a subscriber unit in a telecommunications system, being removably connected to

a transceiver (6) of the subscriber unit, and comprising a multiplicity of fixed memory locations (22, 24), and means responsive to the detection of a message transmitted remotely thereto to store the message in a selected one of the fixed memory locations.

13. A module (7) as claimed in claim 12, wherein at least one of the fixed memory locations (22, 24) is protected from overwriting from the subscriber unit.

14. A module (7) as claimed in claim 12 or 13, including means (27, 28) for rendering any or all of said fixed memory locations accessible or inaccessible from either the subscriber unit or the host station.

15. A module (7) as claimed in claim 12, 13 or 14, including a directory structure (21) within which files can be stored.

16. A module (7) as claimed in any one of claims 12 to 15, wherein the module is in the form of an integrated circuit card.

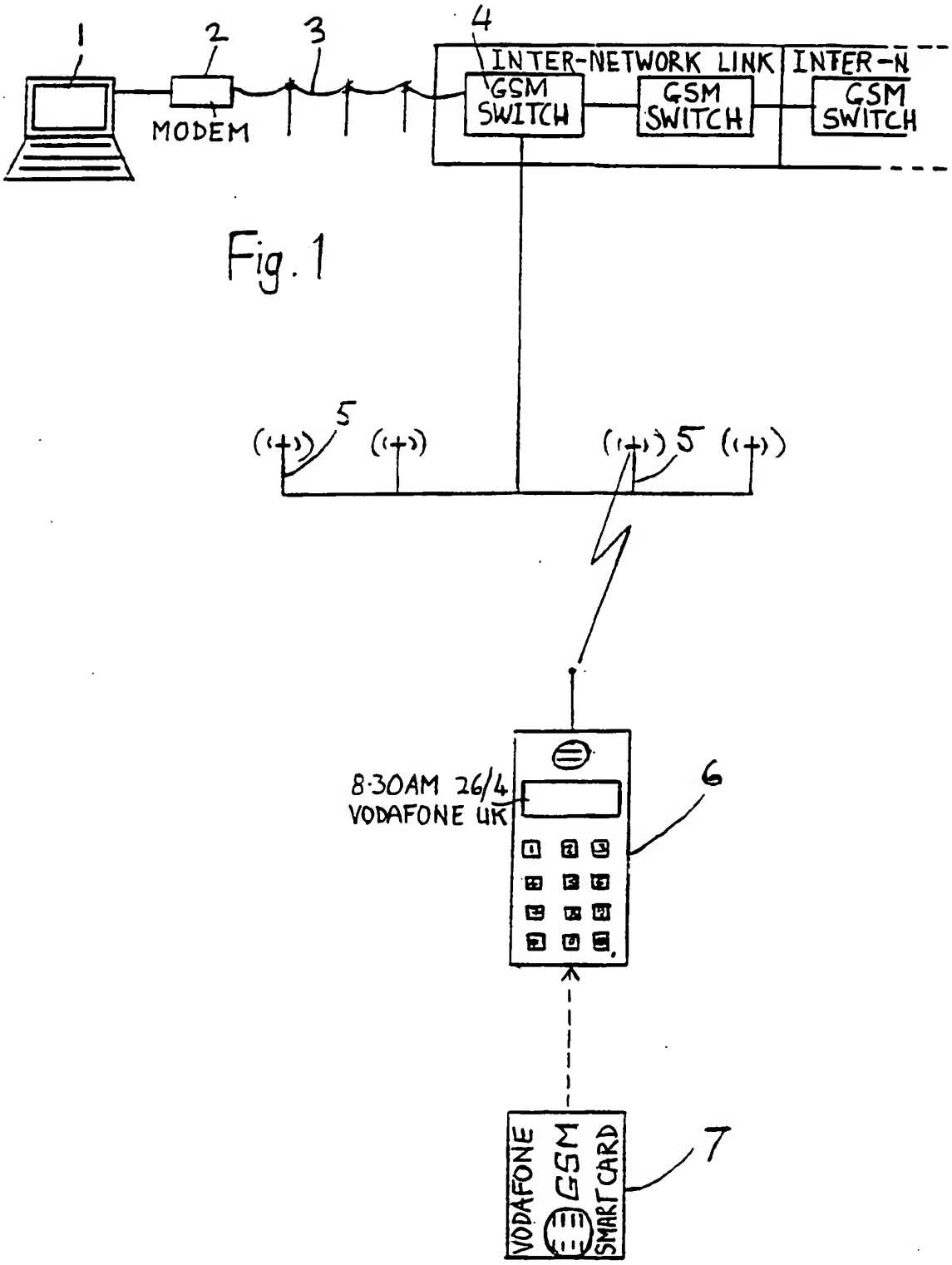

1
2
3
4
MODEM
INTER-NETWORK LINK
INTER-N
GSM SWITCH
GSM SWITCH
GSM SWITCH
5
5
8·30AM 26/4
VODAFONE UK
6
VODAFONE
GSM
SMART CARD
7

Fig. 1

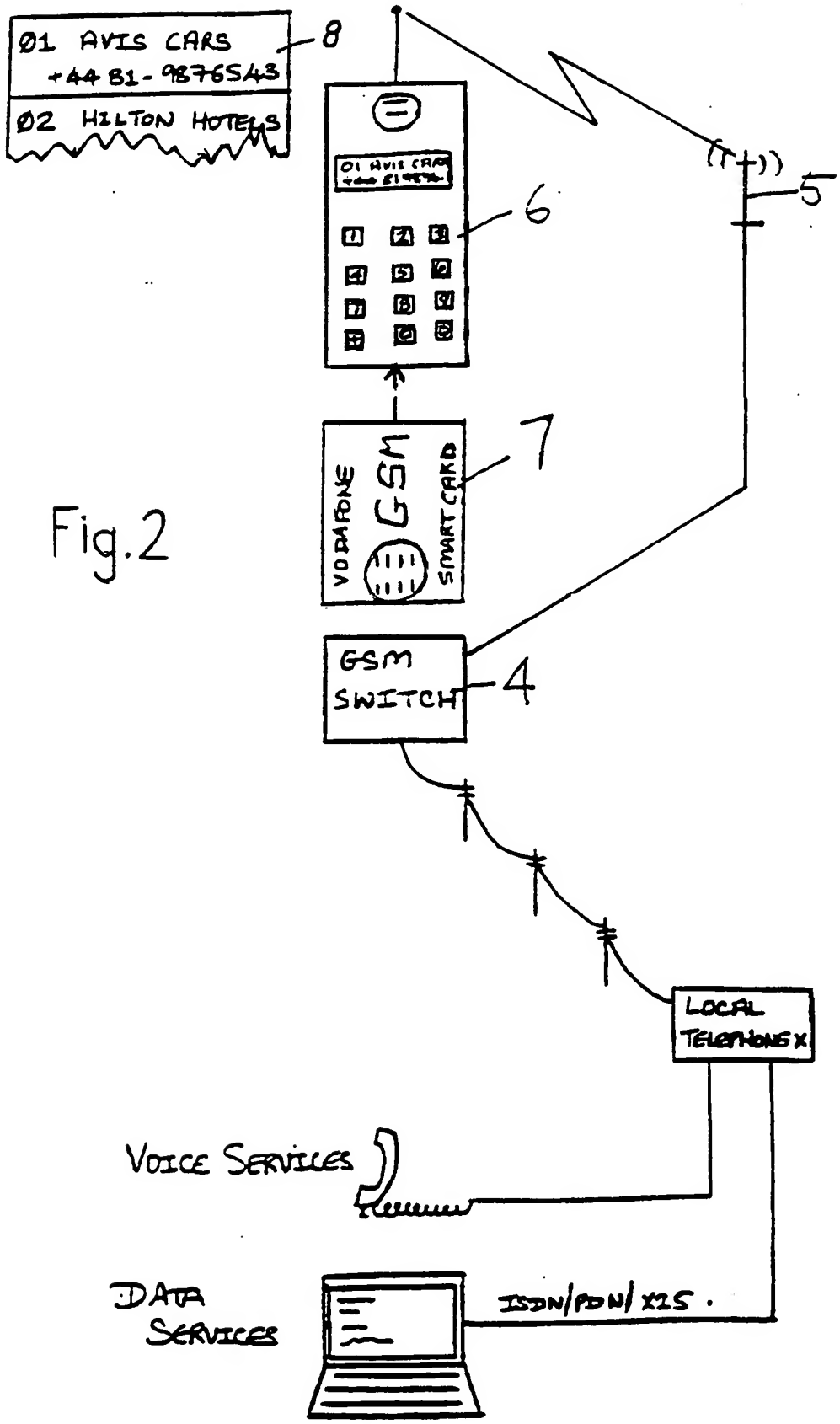
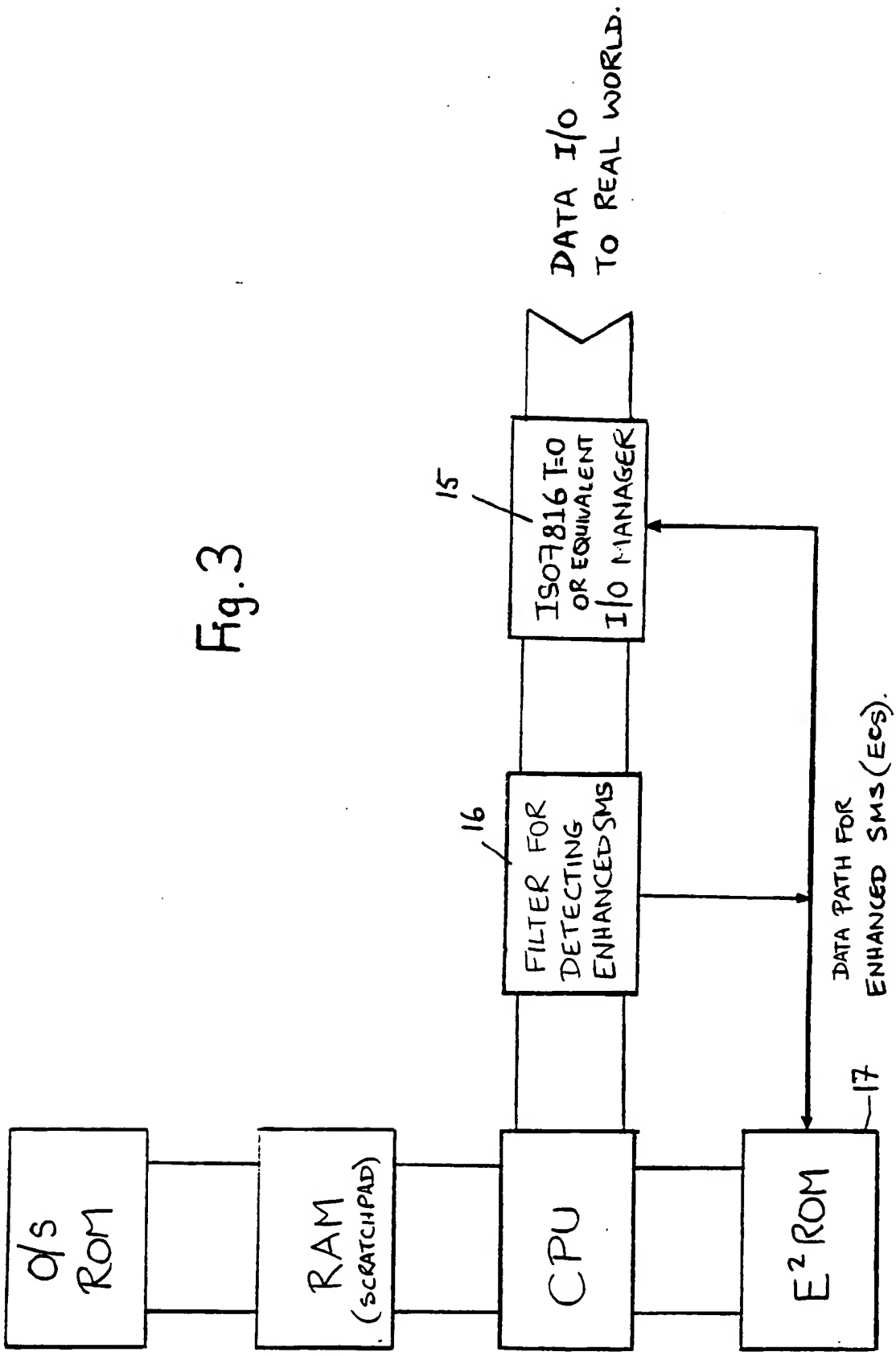



Fig.2

Fig. 3


DATA I/O
TO REAL WORLD.
15
ISO7816 T=0
OR EQUIVALENT
I/O MANAGER
16
FILTER FOR
DETECTING
ENHANCED SMS
DATA PATH FOR
ENHANCED SMS (ECS).
17
O/S
ROM
RAM
(SCRATCHPAD)
CPU
E²ROM

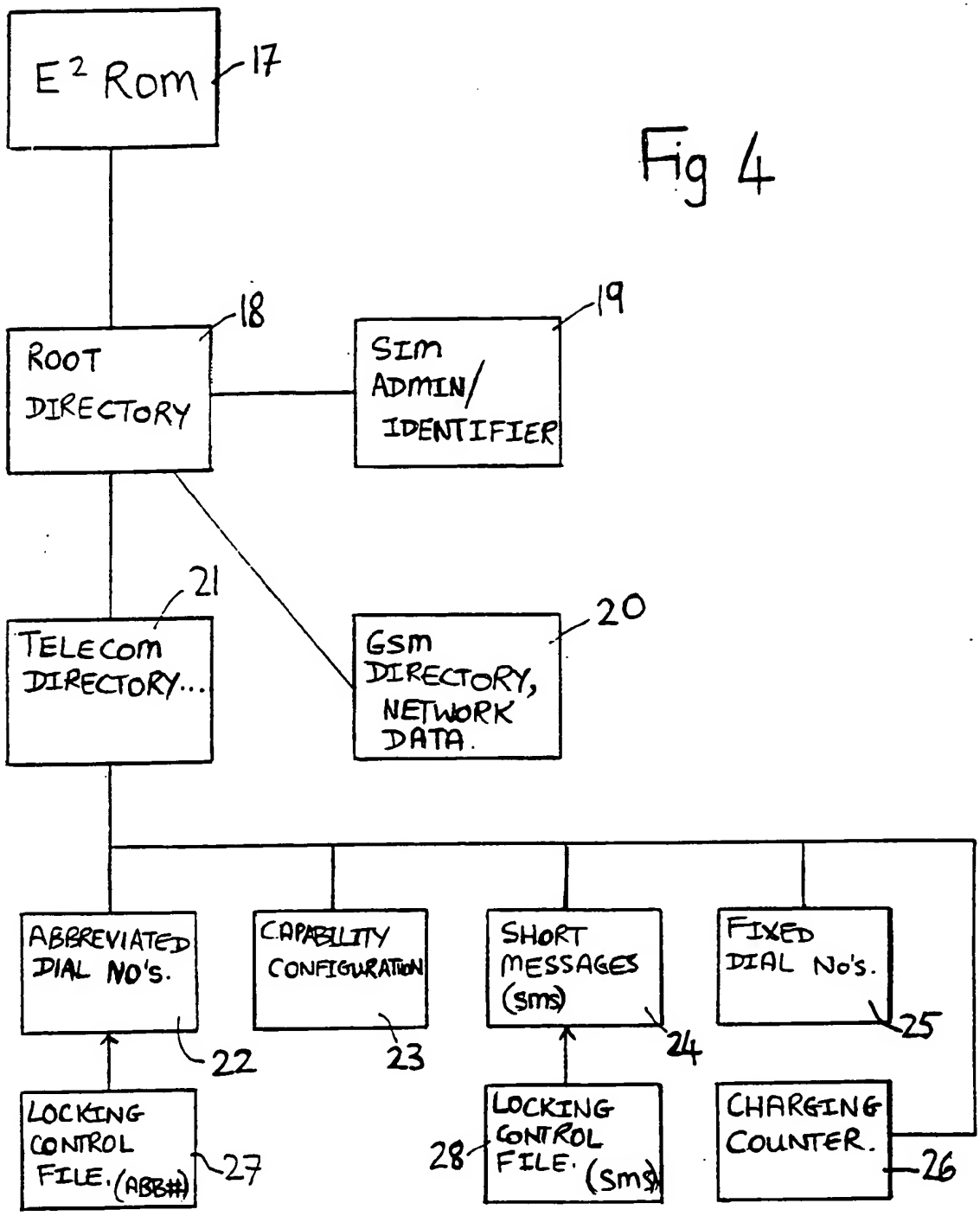



Fig 4

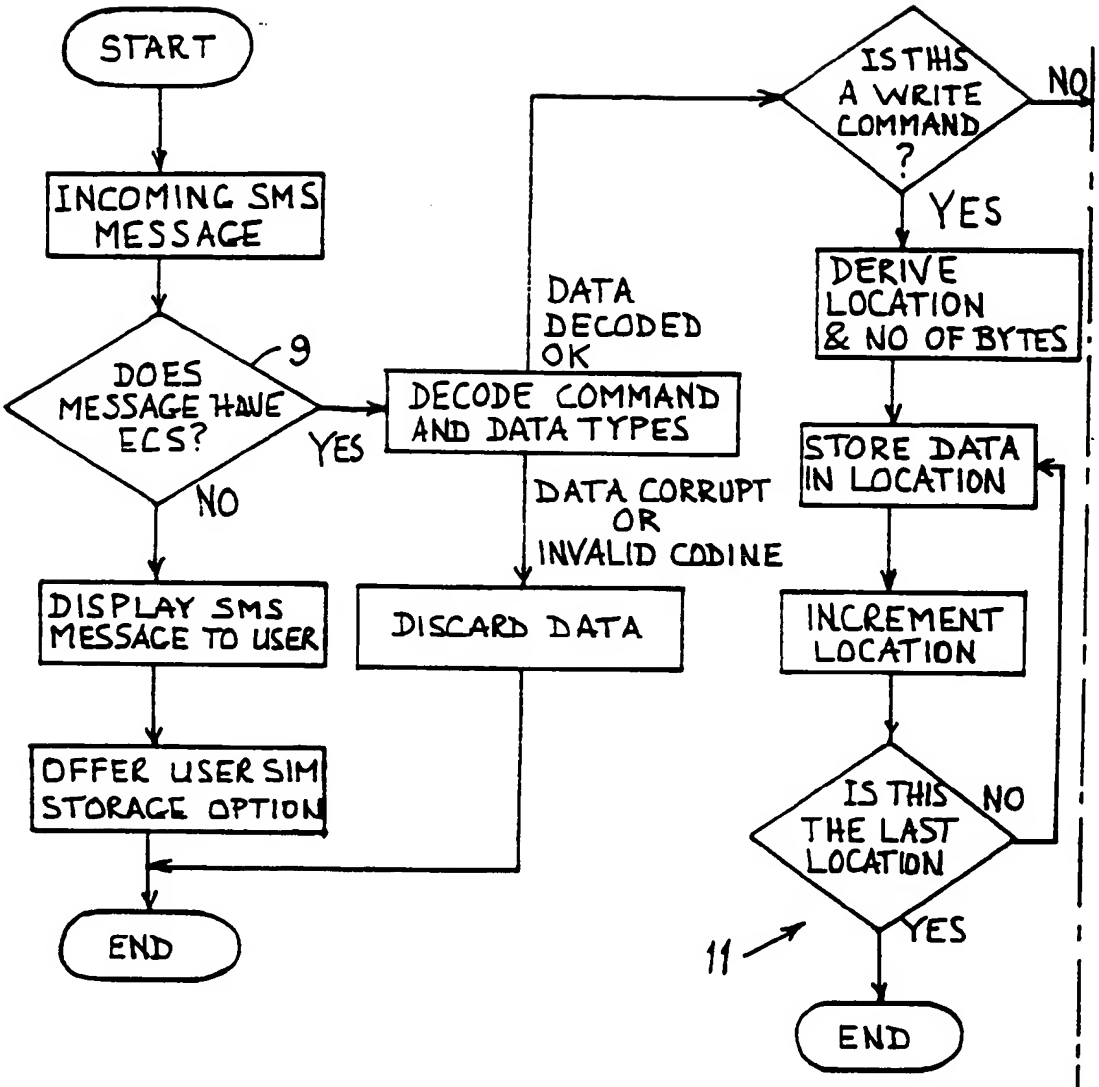

START
INCOMING SMS MESSAGE
DOES MESSAGE HAVE ECS?
9
YES
NO
DISPLAY SMS MESSAGE TO USER
OFFER USER SIM STORAGE OPTION
END
DECODE COMMAND AND DATA TYPES
DATA DECODED OK
DATA CORRUPT OR INVALID CODINE
DISCARD DATA
IS THIS A WRITE COMMAND ?
NO
YES
DERIVE LOCATION & NO OF BYTES
STORE DATA IN LOCATION
INCREMENT LOCATION
IS THIS THE LAST LOCATION
NO
YES
11
END

Fig.5

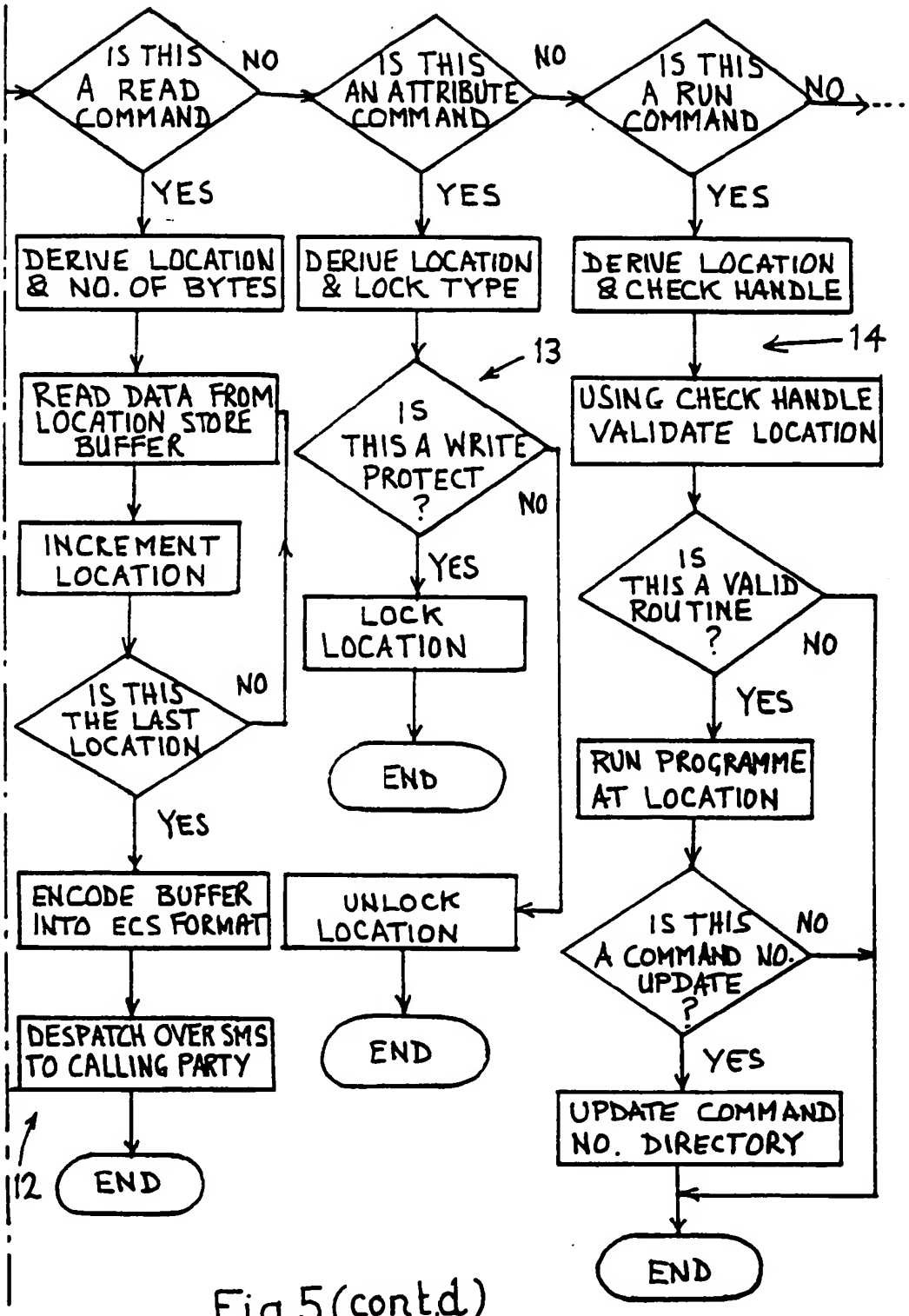

IS THIS A READ COMMAND
NO
IS THIS AN ATTRIBUTE COMMAND
NO
IS THIS A RUN COMMAND
NO
YES
YES
YES
DERIVE LOCATION & NO. OF BYTES
DERIVE LOCATION & LOCK TYPE
DERIVE LOCATION & CHECK HANDLE
13
14
READ DATA FROM LOCATION STORE BUFFER
IS THIS A WRITE PROTECT ?
NO
USING CHECK HANDLE VALIDATE LOCATION
INCREMENT LOCATION
YES
IS THIS A VALID ROUTINE ?
NO
LOCK LOCATION
IS THIS THE LAST LOCATION
NO
YES
END
YES
RUN PROGRAMME AT LOCATION
ENCODE BUFFER INTO ECS FORMAT
UNLOCK LOCATION
IS THIS A COMMAND NO. UPDATE ?
NO
DESPATCH OVER SMS TO CALLING PARTY
END
YES
UPDATE COMMAND NO. DIRECTORY
12
END
END

Fig.5(cont.d)